CSP Vulnerability Scanner™

CSP VulScan is a vulnerability scanning and reporting solution for HPE NonStop systems. This tool helps identify vulnerabilities by checking the NonStop system configuration, access permissions, and security settings. It generates insightful reports for users and recommends changes to improve the security posture.

To effectively audit the security of the systems, the CSP Vulnerability Scanner gathers a vast amount of information from different sources, including Safeguard, Guardian, and other subsystems. It automates this task by providing insightful reports for technical and non-technical users.

CSP Vulnerability Scanner v3.0 can now scan Pathways and the OSS environment. It is now enhanced with several new OSS and Pathway reports.

What's New in Version 3.0

New OSS Reports in v3.0:

- OSS File Verification Report
- OSS User Access Report
- OSS Orphan Files Report
- OSS SetUID/SetGID report
- OSS Directory Contents report
- OSS Symbolic Links report

New Pathway Reports in v3.0:

- Pathway Files Report: List files containing Pathway commands and TPS objects.
- Compare History of Pathway Files:
  - Summary report of Pathway files added/deleted between two reports.
  - Details report of Pathway files added/deleted between two reports.

Key Features

- Scans NonStop systems to identify vulnerabilities
- Provides recommendations to improve security
- Very easy to install and use
- Quickly perform scans and generate insightful reports
- Easily select from list of available reports
- Export reports with Spoolview
- Share reports with management and auditors

Types of Reports

- Security Analysis Report
- Authorization Report
- Examine Sub-volume Access Report
- Explain Access to Object Report
- Group Members Report
- Show Access Report
- Safeguard Globals Report
- Object Verification Report
- New Program Discovery Report
- Orphan Files Report
- Weak Passwords Report

CSP Vulnerability Scanner™

Installation & Use

The installation process is quick, and the solution is easy to use. There are two ways to select the desired scans & generate reports:

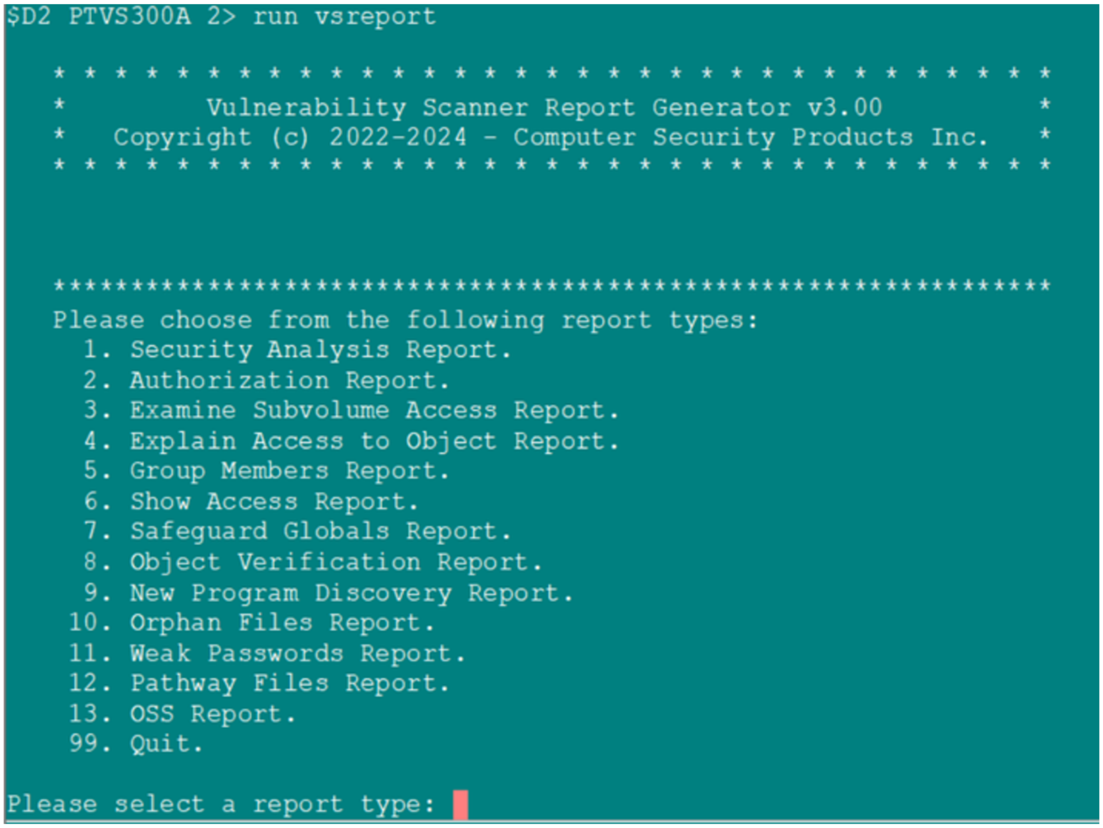
a)VSREPORT Macro- This TACL macro guides the users to build a report

b)TACL command line – For users that are very familiar with command syntax

The users will be able to select from a list of available reports and, based on the selection, may be prompted for some additional information.

Report Types

Execute the VSREPORT macro from the installation sub-volume. It presents 13 key report categories for selection.



```
$D2 PTVS300A 2> run vsreport

   * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *
   *         Vulnerability Scanner Report Generator v3.00            *
   *   Copyright (c) 2022-2024 - Computer Security Products Inc.     *
   * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * *



   *****************************************************************
   Please choose from the following report types:
     1. Security Analysis Report.
     2. Authorization Report.
     3. Examine Subvolume Access Report.
     4. Explain Access to Object Report.
     5. Group Members Report.
     6. Show Access Report.
     7. Safeguard Globals Report.
     8. Object Verification Report.
     9. New Program Discovery Report.
    10. Orphan Files Report.
    11. Weak Passwords Report.
    12. Pathway Files Report.
    13. OSS Report.
    99. Quit.

Please select a report type: 
```